DTE Firewalls

Dan Sterne
sterne@tis.com

Lee Badger
badger@tis.com

Trusted Information Systems, Inc.
3060 Washington Road (Rt. 97)
Glenwood, MD 21738

http://www.tis.com/docs/Research/dtefw.html
http://www.tis.com/docs/Research/DTE.html

Problem

Many organizations are connecting to Internet in spite of security risks

Firewalls help, but are not enough:

- too many services must be restricted (e.g., NFS, X11)
- security perimeter is inflexible
- no protection of sensitive data
- no protection from inside attacks
- limited protection from content-based attacks (e.g., Java)

Need supporting security from operating system (OS), but ...

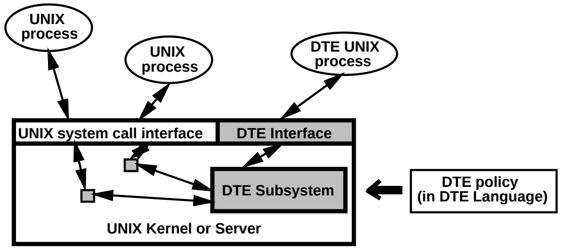
- mainstream OSs (e.g. UNIX) provide only weak, discretionary mechanisms
- MLS OSs strong but inflexible

Solution Strategy

Combine three technologies:

- Internet Firewalls - regulate and filter services
- Domain and Type Enforcement (DTE) - secure UNIX
- Cryptography - protect communications over Internet

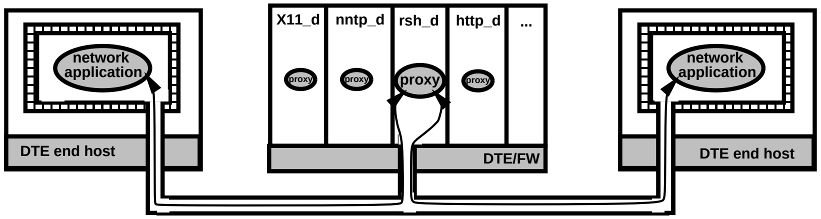
Domain and Type Enforcement (DTE) *



- Strong, flexible access control for operating systems
- Security policies specified in high-level DTE Language (DTEL)
- Backward compatible with UNIX programs, TCP/IP networks.
- Labels and mediates network messages.

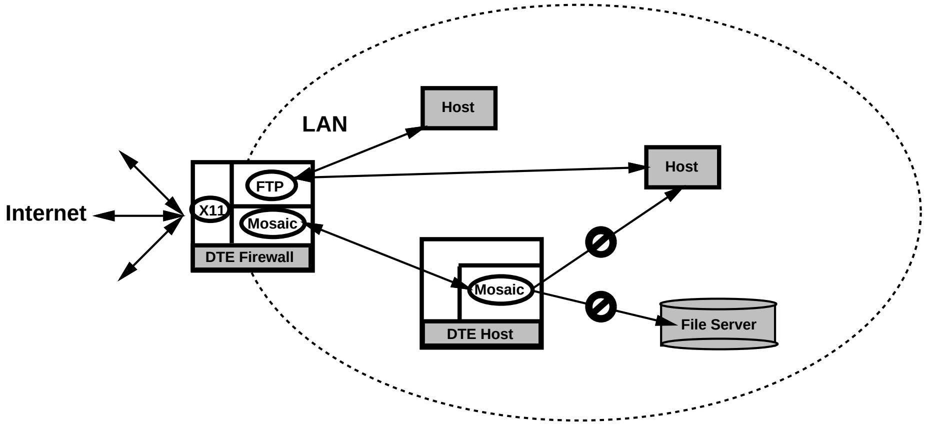
* An extension of Boebert and Kain's Type Enforcement

DTE Firewall Strategy



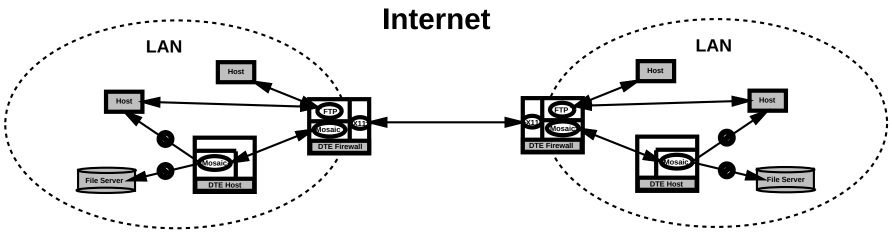
- DTE hosts confine applications
- DTE firewalls:
  - coordinate DTE policies between DTE hosts
  - associate DTE attributes with data from non-DTE hosts
  - confine network proxies

Phase 1: DTE Firewalls



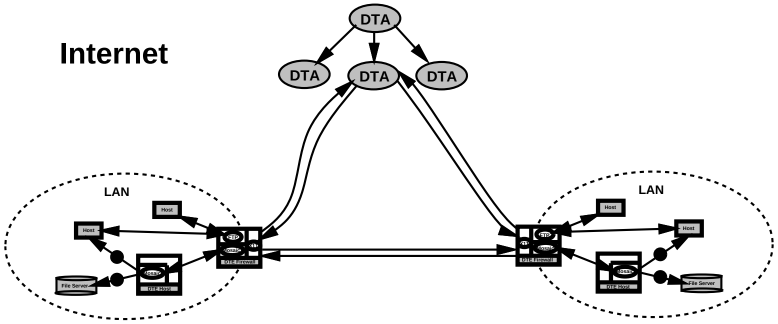
- Safely use more network services
- Stronger firewalls
- Encapsulated network processes
- Protects sensitive information

Phase 2: Distributed DTE Firewalls



- Encryption between Firewalls
- Restricted environments span LANs
- Coordinated protection via DTEL

Phase 3: Domain and Type Authority (DTA)



- Establishes trust relationships
- Provides authentication
- Distributes DTEL modules
- Dynamic policy discovery service